

Ser. No.: 10/629,038
Atty Docket: 42P16118

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:) Examiner: Samson B. LEMMA
)
Mallik Bulusu) Confirmation No.: 7385
)
Application No.: 10/629,038) Art Unit: 2132
Docket No.: 42P16118)
)
Filed: July 28, 2003)
)

For: METHOD AND APPARATUS FOR TRUSTED
BLADE DEVICE COMPUTING

ELECTION AND PRELIMINARY AMENDMENT

Mail Stop Non Fee Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In response to the Restriction Requirement mailed on April 4, 2007, please reconsider
the pending claims based on the following amendments and remarks.

Amendments to the Claims

1. (original) A system comprising:
a blade device; and
chassis management logic, the chassis management logic to determine whether one or more capabilities associated with the blade device match a capability policy.
2. (original) The system of claim 1, further comprising:
a data communication pathway coupled to the blade device and to the chassis management logic.
3. (original) The system of claim 1, wherein:
the chassis management logic is further to isolate the blade device from a computing domain responsive to determining that the blade device capabilities do not match the capability policy.
4. (original) The system of claim 1, further comprising:
a plurality of blade devices;
wherein each of the plurality of blade devices is coupled to the data communication pathway; and
wherein the chassis management logic is further to determine, for at least one of the plurality of blade devices, whether blade capabilities associated with the at least one blade device match the capability policy.
5. (original) The system of claim 4, wherein:
the chassis management logic is further to isolate from the computing domain any of the plurality of blade devices whose associated capabilities do not match the capability policy.

6. (original) The system of claim 1, wherein:
the chassis management logic is further to determine whether the blade device is trusted.

7. (original) The system of claim 1, further comprising:
a baseboard memory controller, wherein the baseboard memory controller is to control communication between the blade device and the chassis management logic.

8. (original) The system of claim 1, wherein:
the blade device includes logic to perform boot processing.

9. (original) The system of claim 8, wherein:
the chassis management logic is further to generate a failure indicator value responsive to determining that the blade device capabilities do not match the capability policy; and
the blade device is to, responsive to the failure indicator value, terminate the boot processing.

10. (original) The system of claim 1, further comprising:
a chassis to receive the blade device.

11. (original) A method comprising:
determining if one or more capabilities associated with a blade device match a capability policy; and
if the blade device capabilities do not match the capability policy, isolating the blade device from a computing domain.

12. (original) The method of claim 11, further comprising:
challenging the blade device to provide a response; and

if the blade device does not provide the response, isolating the blade device from the computing domain.

13. (original) The method of claim 11, wherein determining further comprises:
accessing a capability record associated with the blade.

14. (original) The method of claim 11, further comprising:
maintaining in a central repository a plurality of capability records, each capability record being associated with one of a plurality of blade devices.

15. (original) The method of claim 12, wherein challenging further comprises:
encrypting a challenge value using a public key value; and
providing the encrypted challenge value to the blade device.

16. (original) The method of claim 11, further comprising:
maintaining in a central repository a plurality of public key values, each of the public key values corresponding to one of a plurality of blade devices.

17. (original) An article comprising:
a machine-readable storage medium having a plurality of machine accessible instructions, which if executed by a machine, cause the machine to perform operations comprising:
registering one or more capabilities with a central repository;
determining if one or more capabilities associated with a blade device match a capability policy; and
if the blade device capabilities do not match the capability policy, isolating the blade device from a computing domain.

18. (original) The article of claim 17, further comprising:
a plurality of machine accessible instructions, which if executed by a machine, cause the machine to perform operations comprising:
challenging the blade device to provide a response; and
if the blade device does not provide the response, isolating the blade device from the computing domain.

19. (original) The article of claim 17, wherein:
the instructions that cause the machine to determine if one or more capabilities associated with a blade device match a capability policy further comprise instructions that cause the machine to access a capability record associated with the blade.

20. (original) The article of claim 17, further comprising:
a plurality of machine accessible instructions, which if executed by a machine, cause the machine to perform operations comprising:
maintaining in a central repository a plurality of capability records, each capability record being associated with one of a plurality of blade devices.

21. (original) The article of claim 18, wherein:
the instructions that cause the machine to challenge further comprise instructions that cause the machine to :
encrypt a challenge value using a public key value; and
provide the encrypted challenge value to the blade device.

22. (original) The article of claim 17, further comprising:
a plurality of machine accessible instructions, which if executed by a machine, cause the machine to perform operations comprising:
maintaining in a central repository a plurality of public key values, each of the public key values corresponding to one of a plurality of blade devices.

23. (original) A method comprising:
registering one or more capabilities with a central repository;
determining if a capability authorization has been received within a pre-defined timeout interval;

if the capability authorization has been received within the timeout interval,
performing boot processing; and

if the capability authorization has not been received within the timeout interval,
declining to perform the boot processing.

24. (original) The method of claim 23, further comprising:

providing a response to a challenge;
proceeding, if the response is correct, with boot processing; and
if the response is not correct, isolating from a computing domain.

25. (original) The method of claim 24, wherein:

providing a response further comprises decrypting a challenge value using a private key.

26. (original) The method of claim 23, wherein:

declining to perform the boot processing further comprise performing stand-alone boot processing.

27. (original) The method of claim 23, wherein:

declining to perform the boot processing further comprises powering down.

28. (original) An article comprising:

a machine-readable storage medium having a plurality of machine accessible instructions, which if executed by a machine, cause the machine to perform operations comprising:

registering one or more capabilities with a central repository;

determining if a capability authorization has been received within a pre-defined timeout interval;

if the capability authorization has been received within the timeout interval, performing boot processing; and

if the capability authorization has not been received within the timeout interval, declining to perform the boot processing.

29. (original) The article of claim 23, further comprising:

a plurality of machine accessible instructions, which if executed by a machine, cause the machine to perform operations comprising:

providing a response to a challenge;

proceeding, if the response is correct, with boot processing; and

if the response is not correct, isolating from a computing domain.

30. (original) The article of claim 24, wherein:

instructions that cause the machine to provide a response further comprise instructions that cause the machine to decrypt a challenge value using a private key.

31. (original) The article of claim 23, wherein:

instructions that cause the computer to decline to perform the boot processing further comprise instructions that cause the machine to perform stand-alone boot processing.

32. (original) The article of claim 23, wherein:

instructions that cause the computer to decline to perform the boot processing further comprise instructions that cause the machine to power down.

33. (newly added) The system as recited in claim 1, wherein the chassis management logic further comprises authentication logic to determine whether the blade device is to be authenticated before determining whether one or more capabilities associated with the blade device match the capability policy.

34. (newly added) The system as recited in claim 1, wherein the chassis management logic is to register the one or more capabilities associated with the blade device with a central repository, and determine whether the one or more registered capabilities associated with the blade device match the capability policy, resulting in a capability authorization;

if the capability authorization has been received within a predetermined timeout interval, the chassis management logic to allow boot processing of the blade device; and

if the capability authorization has not been received within the predetermined timeout interval, then the chassis management logic to disallow the boot processing of the blade device.

REMARKS

Reconsideration of the above referenced application in view of the enclosed amendments and remarks is requested. Claims 33 and 34 have been added to recite additional features of the claimed embodiments.

ELECTION:

The Examiner has noted that the application contains claims directed to two patentably distinct species, namely:

Group I. Claims 1-22, drawn to a system comprising a blade device; and chassis management logic, the chassis management logic to determine whether one or more capabilities associated with the blade device match a capability policy.

Group II. Claims 23-32, drawn to a method comprising: registering one or more capabilities with a central repository; determining if a capability authorization has been received within a pre-defined timeout interval; if the capability authorization has been received within the timeout interval, performing boot processing; and if the capability authorization has not been received within the timeout interval, declining to perform the boot processing.

In response to the restriction requirement, Applicants hereby elect Group I comprising Claims 1 to 22, with traverse. Newly added Claims 33 and 34 should be included in Group I, as being dependent on Claim 1.

First, Applicants respectfully submit that the restriction is improper. Second, even assuming the restriction is made final, Applicants believe that they are entitled to examination of additional claims. Specifically, Claims 33 and 34 are added and dependent on Claim 1 (Group I). It should be further noted, that Claim 34 is similar in scope and features to Claim 23. Therefore, any search for features in Group I would be co-extensive with a search for Group II.

Without admitting or denying the foundation for Examiner's assertion that the two groups are patentably distinct, Applicants stress that the Examiner has failed to meet the burden of the test for requiring a restriction. The Examiner readily admits that the two groups are searchable in the same Class. The Examiner also fails to provide sufficient reason for restricting the two groups other than a recitation of the claim language of two independent claims. Both Groups are directed toward embodiments of an invention that uses capabilities associated with a blade device, and a determination of whether the capabilities either match a policy or authorization. It is suggested that a search for the elements of one group would encompass a search for elements recited in the other group.

Applicants respectfully submit that the restriction is improper. First, the Examiner has provided little explanation in support of the restriction requirement beyond generic boilerplate paragraphs. As set forth in MPEP § 808, "*Every requirement to restrict has two aspects:*

(A) the reasons (as distinguished from the mere statement of conclusion) why the inventions as claimed are either independent or distinct; and

(B) the reasons for insisting upon restriction therebetween..."

Further, for a restriction requirement to be proper according to MPEP § 803, citing MPEP § 806.04 and 806.05, under the statute an application may properly be required to be restricted to one of two or more claimed inventions only if they are able to support separate patents and they are either independent or distinct. However, "*if the search and examination of an entire application can be made without serious burden, the examiner must examine it on the merits, even though it includes claims to independent or distinct inventions.*" MPEP § 803. Here, Applicants note no substantial distinctions between Groups I and II which would necessitate a serious burden. Indeed, both groups are related to capabilities associated with blade servers, and the difference between the groups substantially being the method of determination of either authorization or policy matching.

Additionally, it is not seen how one could limit search terms to search for only one species of the claimed invention without finding relevant prior art in all of the species of embodiments, if such art exists. Thus, no serious burden exists for the Examiner.

Further, the burden on the Applicants is believed to outweigh any burden there may be on the Examiner to search various embodiments of the invention, particularly since the searches would be co-extensive. Restriction would be unduly burdensome to Applicants, not only in time, but also in money, particularly considering the current filing and maintenance fee schedules.

Considering these factors, it is respectfully submitted that the restriction requirement is improper since Groups I and II are indeed related. Moreover, the Examiner is respectfully requested to weigh the great burden a restriction would have on Applicants and withdraw the restriction requirement.

In view of the foregoing, it requested that restriction requirement be reconsidered, and examination on the merits to proceed. Please charge any shortage of fees in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-0221 and please credit any excess fees to such account.

Respectfully submitted,

Dated: 25 April 2007

/ Joni D. Stutman-Horn /
Joni D. Stutman-Horn, Reg. No. 42,173
Patent Attorney
Intel Corporation
(703) 633-6845

Intel Corporation
c/o Intellevate, LLC
P.O. Box 52050
Minneapolis, MN 55402